APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/663,664	09/15/2000	David M. Chess	YOR920000457US1(13807)	2186

7590   03/08/2005

Richard L Catania
Scully Scott Murphy & Presser
400 Garden City Plaza
Garden City, NY 11530

EXAMINER
COLIN, CARL G

ART UNIT	PAPER NUMBER
2136	

DATE MAILED: 03/08/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

PTO-90C (Rev. 10/03)

	Application No.	Applicant(s)
Office Action Summary	09/663,664	CHESS ET AL.
	Examiner	Art Unit
	Carl Colin	2136

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) FROM
THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed
  after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any
  earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on <u>03 December 2004</u> .

2a)☒ This action is **FINAL**.   2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is
closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) <u>1-42</u> is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) <u>1-42</u> is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on <u>15 September 2000</u> is/are: a)☒ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11)☐ The proposed drawing correction filed on _____ is: a)☐ approved b)☐ disapproved by the Examiner.

    If approved, corrected drawings are required in reply to this Office action.

12)☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

13)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All b)☐ Some * c)☐ None of:

      1.☐ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____ .

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage
application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

    a) ☐ The translation of the foreign language provisional application has been received.

15)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

1)☒ Notice of References Cited (PTO-892)

2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3)☐ Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____ .

4)☐ Interview Summary (PTO-413) Paper No(s). _____ .

5)☐ Notice of Informal Patent Application (PTO-152)

6)☐ Other: .

DETAILED ACTION

Response to Arguments

1.   . In response to communications filed on 12/3/2004, applicant has amended claims 1, 10-

14, 16, 17, 22, 28-31, 33-34, 37, 39, 40. The following claims 1-42 are presented for

examination.

2.   The amendments to the specification, page 2, filed on 12/3/2004 have been considered

and the objection has been withdrawn. The objection to the drawings has been withdrawn with

respect to the amended specifications. The 35 USC 112 rejection has been withdrawn with

respect to the amended claims.

3.   Applicant's arguments, pages 15-20, filed on 12/3/2004, with respect to the rejection of

claims 1-42 have been fully considered, but they are not persuasive. Applicant amends the

independent claims to add the limitation of "using a trusted co-server as a trusted third party in

interactions between the client and the server". Applicant argues that the reference does not

teach the prior art as amended because there is no means involved for any party to verify that the

information at the other end is protected. However, Iwamura discloses several embodiments

where the agency is used as a trusted third party in interactions between the client and the server.

For example column 9, lines 32-35 recite that the agency provides the user and the shop with

signature key and verification means and user and shop (server) generate signature key and

verifying key (column 9, lines 39-50). Iwamura discusses in (column 9, lines 50-67) the digital

signature verifying keys generating by the agency for both the user and the server. Iwamura further discloses in (column 10, lines 19-67) interactions between the user and the server using the agency as a trusted third party wherein the co-server executes so that parties can authenticate and trust the correct execution of the co-server as claimed in claim 34. Regarding claim 37, Iwamura discloses the limitation of the co-server carrying out a function on inputs such that the parties trust interactions between the parties and the server (column 11, lines 15-45). In view of the above, applicant has not overcome the prior art, and independent claims 1, 31, 33, 34, 37, and 40 as amended are still rejected under the same ground of rejection. Examiner maintains the sme ground of rejection of claims 1-42 under 35 USC 103 (a). The rejection of the dependent claims not challenged by applicant still applies in this office action.

Claim Rejections - 35 USC § 112

4.   The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter, which the applicant regards as his invention.

Claim 34 and the intervening claims are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

4.1   **Claim 34** recites the limitation "between the client and the server". There is insufficient antecedent basis for this limitation in the claim. It is not definite whether "the server" refers to the web server or the co-server.

Claim Rejections - 35 USC § 103

5.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or

described as set forth in section 102 of this title, if the differences between the subject matter

sought to be patented and the prior art are such that the subject matter as a whole would have

been obvious at the time the invention was made to a person having ordinary skill in the art to

which said subject matter pertains. Patentability shall not be negatived by the manner in which

the invention was made.

5.1   **Claims 1-5, 7-23, 26-42** are rejected under 35 U.S.C. 103(a) as being unpatentable over

US Patent 6,453,296 to **Iwamura** in view of Non-Patent Literature: **Wilhelml, U., et al.**

"Introducing Trusted Third Parties to the Mobile Agent Paradigm" Institute pour les

Communications informatiques et leurs Applications, Ecole Polytechnique Fédérale de

Lausanne, 1015 Lausanne, Switzerland, Pages 1-21.

5.2   **As per claims 1, 2, 4, 7, 31, 33, 34, 35, 37, 38, 40, and 41, Iwamura** substantially

teaches a method, comprised of enhancing a computational service to each client of a plurality of

clients, by: moving a selected portion of a computation from a server into a trusted co-server;

and allowing each client to interact with the server and the co-server, for example (see column 4,

lines 21-52 and column 9, lines 20-67). **Iwamura** further teaches multiple parties interaction

(see column 3, lines 45-67). **Iwamura** discloses several embodiments where the agency is used

as a trusted third party in interactions between the client and the server. For example, column 9, lines 32-35 recite that the agency provides the user and the shop with signature key and verification means and user and shop (server) generate signature key and verifying key (column 9, lines 39-50). **Iwamura** discusses in (column 9, lines 50-67) the digital signature verifying keys generating by the agency for both the user and the server. **Iwamura** further discloses in (column 10, lines 19-67) interactions between the user and the server using the agency as a trusted third party wherein the co-server executes so that parties can authenticate and trust the correct execution of the co-server as claimed in claim 34. Regarding claim 37, **Iwamura** discloses the limitation of the co-server carrying out a function on inputs such that the parties trust interactions between the parties and the server (column 11, lines 15-45). **Iwamura** does not explicitly disclose that the trusted co-server is executing inside a secure coprocessor. Secure coprocessors are well known in the art for providing tamper resistant hardware protection. **Wilhelml et al.** in an analogous art teaches moving computation from a server into a trusted co-server controlled by an operator, executing inside a secure coprocessor to provide a trustworthy environment, for example (see sections 5-6). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of **Iwamura** to move a selected portion of a computation from a server into a trusted co-server in order to provide a trustworthy environment as taught by **Wilhelml et al.**. This modification would have been obvious because one skilled in the art would have been motivated by the suggestions provided by **Wilhelml et al.** so as to provide a trustworthy environment.

As per claims 3, 5, 39, and 42, **Iwamura** discloses the limitation of wherein said step of allowing includes enabling said client an authenticated, private channel to said co-server, for example (see column 3, line 45 through column 4, line 52). **Iwamura** discloses the client authenticates the co-server, the client sends its input to the co-server over a private channel, such as one established by encryption with a shared secret key, the co-server sends its output to said another party over a private channel, such as one established by encryption with a shared secret key, for example (see columns 10-11 and summary).

As per claims 8 and 9, **Iwamura** discloses the limitation of wherein said step of enhancing includes providing a desired security and/or privacy property, wherein said step of enhancing includes providing at least one security and/or privacy property to an application selected from the group including: authentication of clients, nonrepudiation of client activity, nonrepudiation of server activity, credit card transaction security, taxes on e-commerce activity, re-selling of intellectual property, privacy of sensitive or proprietary web activity, correctness of web activity, enforcement of logo and/or "seal of approval" licenses, safety of downloadable content, authenticity of downloadable content, integrity of server machine, and any combination of these, for example (see column 1, line 40 through column 3, line 15; and column 3, line 45 through column 4, line 52).

As per claims 10-12, **Iwamura** discloses co-server algorithm that generates output that includes a signed statement using a private key known to the co-server and discloses authenticating both the client and the server, for example (see columns 9-10). **Wilhelml et al.**

discloses generating output based on current agent state that meets the recitation of wherein input
from said client is prompt from server for the user's private authenticator data, such as a
password, input from said server is this authentication data, co-server algorithm, that generates
output to said client based on said current co-server state and said inputs indicates whether or not
the authenticator data is correct for this user, and generates output to said client based on said
current co-server state and said inputs includes a signed statement, using a privacy key known to
the co-server, attesting, for the client, that the server engaged in an interaction satisfying certain
properties, for example (see sections 2.1 and 4.3). Therefore, these claims are rejected on the
same rejection as claim 1.

As per claims 13-16, Iwamura discloses the limitation of wherein: the client's input
includes a credit card number (CCN), the output co-server algorithm that generates output to said
client based on said current co-server state and said inputs includes the CCN, encrypted so that
the server cannot read it but an acquirer can and wherein the server includes a transaction
amount, the output co-server algorithm that generates output to said client based on said current
co-server state and said inputs includes the transaction amount, cryptographically bound to the
encrypted CCN so that the server cannot alter it, for example (see column 9, line 21 through
column 10). Iwamura further discloses protecting the client personal information and the server
information using cryptography and time stamping so that data can be transmitted to the acquirer
in such a manner so that the acquirer can receive this transaction exactly once, for example (see
column 10, line 50 through column 11 and column 12, lines 15-51). Wilhelml et al. also
discloses generating output to said client based on said current co-server state and said inputs

includes the transaction amount, cryptographically bound to the encrypted CCN so that the

server cannot alter it encrypting information. Therefore, these claims are rejected on the same

rejection as claim 1.

As per claims 17 and 20, Iwamura discloses a remote party is an owner of intellectual

property, the server input includes part of this property and generating output that includes

portion of input from said client that the limitation of where: a remote party is an owner of

intellectual property, the server input includes part of this property, encrypted so that only the

co-server can decrypt it, the output function co-server algorithm that generates output to said

client based on said current co-server state and said inputs to the client includes a portion of the

decryption of input from said client, for example (see columns 9-12). For instance, column 11,

lines 30 et seq. discloses an example of output to client that includes unencrypted portion and

encrypted information. Column 10 shows a portion of decryption of input that is re-encrypted.

Wilhelml et al. discloses the limitation of except the output function now includes a portion of

the decryption of input from said server, re-encrypted, possibly with rights management rules, in

a manner that a secure coprocessor at the client site can decrypt it, for example (see sections 5.1-

5.2). Therefore, these claims are rejected on the same rejection as claim 1.

Claims 18-19 recites similar limitations as claims 13-16 except for generating a

transformation using a watermark or reducing the quality of plaintext. Such method of hiding

information is well known in the art. Using such method does not depart from the spirit and

scope of the invention disclosed by the above references.

As per claim 21, Iwamura discloses the limitation of wherein: the client input includes a choice of which record R in a set of records the client would like to receive, the co-server includes this record R in its response to the client, however, the co-server obtains R in such a way as the server does not know which record was the one selected, for example (see column 10, lines 39-67 and column 11).

As per claims 22 and 28, Iwamura discloses the limitation of wherein: a remote party establishes a content evaluation scheme, consisting of an evaluation function mapping content to some set of indicators, and as part of computing the client output function co-server algorithm that generates output to said client based on said current co-server state and said inputs, the co-server calculates, or verifies an external calculation, of the evaluation function and includes the result in the client output, for example (see columns 10-11). **Iwamura** discloses verifying a charge and includes the result in client output. See also columns 8-9 for interaction between the devices.

As per claim 23, Iwamura discloses the limitation of where the evaluation function consists of determining whether specified server input from specified server merits a logo or seal of approval, in accordance with a business arrangement between the server and the remote party, for example (see column 9, lines 20 et seq.).

As per claim 26, Iwamura discloses the limitation of using a secure channel and

protecting user information and details of the transaction that meets the recitation of where party

the remote party has injected evaluation function and/or some of its parameters into the co-server

through a private channel, so that the server cannot know the details of the evaluation function

execution occurring on the co-server, for example (see column 8, lines 20-45).

As per claim 27, Iwamura discloses the limitation of where the server input includes

both content and a signature on the content, from one of possibly many content providers, and

the evaluation function includes testing whether the signature is valid, for example (see column

8, lines 50 et seq.).

As per claims 29, 32, and 36, Wilhelml et al. discloses security action s against another

server that meets the recitation of where: the co-server has the ability to carry out

security-enhancing actions against the server, such as booting the server and securely or carrying

out a security scan of the server, the output returned to client indicates which of these actions

have been carried out, and how recently, for example (see sections 4.2 and section 6). It is

apparent to one skilled in the art that the limitation in this claim does not depart from the spirit

and scope of the disclosure of Wilhelml et al.. Therefore claims 29 and 32 are rejected on the

same rationale as the rejection of claim 1.

As per claim 30, Iwamura discloses the limitation of where the client input includes a

message and a specification of the appropriate entities who can read the message, for example

(see columns 10-12). The limitation of encrypted the output based on client input to prevent data

from being read is disclosed by both references as discussed above. The verifying step of

message from the client by the server is also disclosed above. Therefore, **Iwamura** substantially

discloses the limitation of where: the client can specify whether the interaction is a read

interaction or a write interaction; for a write interaction: the client input includes a message M

and a specification S of the appropriate entities who can read this message; the co-server retains

M and S by storing them in some combination across the co-server and server via an algorithm

that generates new co-server state based on said current co-server state and said inputs, the

internal state in the co-server and co-server algorithm that generates output to said server based

on said current co-server state and said inputs; however in said write interaction: any portion of

M sent via co-server algorithm that generates output to said server based on said current

co-server state and said inputs is encrypted, so that the server cannot access the plaintext; and

mechanisms are used to ensure that, when the co-server later retrieves any of this data from the

server, that the data has not been changed; for a read interaction: the client input specifies which

message M the client would like to read, the co-server retrieves S; if the client satisfies S, then

the co-server sends M back to the client, after first retrieving and decrypting it, if necessary, for

example (see columns 10-12).

6.   **Claims 6, 24, and 25** is rejected under 35 U.S.C. 103(a) as being unpatentable over US

Patent 6,453,296 to **Iwamura** in view of Non-Patent Literature: **Wilhelml, U., et al.**

"Introducing Trusted Third Parties to the Mobile Agent Paradigm" Institute pour les

Communications informatiques et leurs Applications, Ecole Polytechnique Fédérale de

Lausanne, 1015 Lausanne, Switzerland, Pages 1-21 as applied to claims 1-19 above, and further in view of US Patent 6,714,982 to **McDonough et al.**.

As per claims 6, 24-25, both references substantially teach the claimed method of claim 1. **Wilhelml et al.** also discloses preventing malicious service. Scanning message for virus before transmission is well known in the art and does not depart from the spirit and scope of the disclosure of **Wilhelml et al.**. Claim 22 is rejected on the same rationale as the rejection as claim 1. **McDonough et al.** in an analogous art teaches determining whether input which has potentially executable content is free of viruses, for example (see column 4, lines 45-55) in order to provide additional security. **McDonough et al.** also discloses where the evaluation function is parameterized by a "signature file" and where the client output includes an identification of which signature file was used in this interaction, for example (see column 4, lines 31 et seq.). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method as combined above to determine whether server input which has potentially executable content is free of viruses in order to provide additional security as taught by **McDonough et al.**. This modification would have been obvious because one skilled in the art would have been motivated by the suggestions provided by **McDonough et al.** in order to provide additional security.

Conclusion

7.   Applicant's amendment necessitated the new ground(s) of rejection presented in this

Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a).

Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from

the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the

mailing date of this final action and the advisory action is not mailed until after the end of the

THREE-MONTH shortened statutory period, then the shortened statutory period will expire on

the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be

calculated from the mailing date of the advisory action. In no event, however, will the statutory

period for reply expire later than SIX MONTHS from the date of this final action.

7.1   The prior art made of record and not relied upon is considered pertinent to applicant's

disclosure as the art discloses the use of co-servers and secured commercial transaction. Many

of the claimed features are disclosed in these references.

US Patents:	5,848,161	Luneau et al.
	5,990,199	Krajewski, Jr. et al.
	6,202,157	Brownlie et al.

US Patent Publication US 2002/0111997   Herlihy

7.1   Any inquiry concerning this communication or earlier communications from the

examiner should be directed to Carl Colin whose telephone number is 571-272-3862. The

examiner can normally be reached on Monday through Thursday, 8:00-6:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the

organization where this application or proceeding is assigned is 703-872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding

should be directed to the receptionist whose telephone number is 703-305-3900.

Ce

Carl Colin

Patent Examiner

March 5, 2005

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100